RSAC 2025 Conference

Many Voices.
One Community.

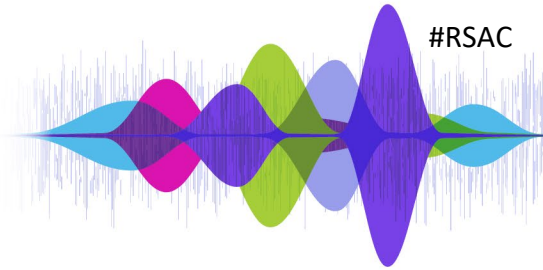
SESSION ID: CIT-M02

Defensive Tensions in Critical Infrastructure Cyber Defense

Joseph Slowik

Founder
Paralus LLC
https://www.linkedin.com/in/joe-slowik/

Disclaimer



Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

Defining “Critical”

“Critical”

critical adjective

crit·i·cal ˈkri-ti-kəl

Synonyms of *critical* ›

1 a : inclined to criticize severely and unfavorably
- Don't be so *critical*. This is just a first attempt.
- They were *critical* of the new policies.

b : consisting of or involving criticism
- *critical* writings

also **:** of or relating to the judgment of critics
- The play was a *critical* success.

c : exercising or involving careful judgment or judicious evaluation
- *critical* thinking
- a *critical* commentary on the mayor's proposal

d : including variant readings and scholarly emendations
- a *critical* edition

2 a : of, relating to, or being a turning point or specially important juncture
- a *critical* decision
- *critical* temperature

b : INDISPENSABLE, VITAL
- a *critical* waterfowl habitat
- a component *critical* to the machine's operation

c : being in or approaching a state of crisis
- a *critical* shortage
- a *critical* situation

d : CRUCIAL, DECISIVE
- a *critical* test

https://www.merriam-webster.com/dictionary/critical

“Critical”

Can Multiple Items be “Critical” at Once?

"Critical"

Can Multiple Items be "Critical" at Once?

Yes – But then Some Items must become "More Critical" than Others!

Critical Infrastructure

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / Topics / Critical Infrastructure Security and Resilience / Resilience Services / Infrastructure Dependency Primer / Learn

SHARE:

Critical Infrastructure Systems

Infrastructure systems are the backbone of communities. While all infrastructure plays a role, some infrastructure systems are more critical than others. Critical infrastructure are those infrastructure systems and assets that are so vital that their incapacitation or destruction would have a debilitating effect on security, the economy, public health, public safety, or any combination thereof.

The U.S. Department of Homeland Security has defined 16 sectors or categories of infrastructure that are considered critical to the nation. At the local level, some of these systems may be owned or operated by local government partners and many of them will be vital to the health, economy, and security of the community or region.

These critical infrastructure sectors are related to and resemble the community lifelines FEMA uses to discuss essential systems within response and recovery operations. Both the sector and lifelines constructs can be used to consider infrastructure dependencies. Within this primer, we will take a closer look at several infrastructure systems that are key to resilience whether looked at through a sector-based or community lifelines lens.

Each critical infrastructure system is made up of individual assets that work together as an integrated system. The figures below illustrate the networking of assets using four of the most important critical infrastructure systems as examples. These four infrastructure sectors—**Energy, Communications, Water, and Transportation**—are critical to the operations of almost all other sectors, as well as each other, and are fundamental to the delivery of the basic societal functions communities seek to provide. While each figure only depicts a single, simplified system within each sector (there are many, and many variations!), they help illustrate the interconnected nature of those systems and their reliance on many individual assets.

Critical Infrastructure Sectors

https://www.preventioninstitute.org/sites/default/files/editor_uploads/5e7921a7b8c4b17eb96991d1_Essential_Critical_Infrastructure_Workers%20.png

Critical Sector Diversity

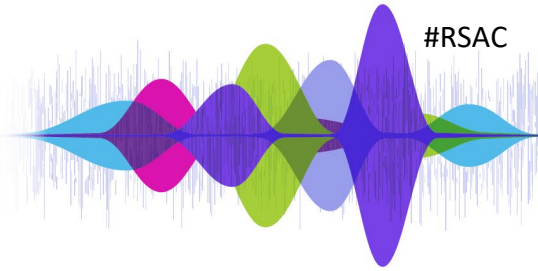
Balancing Between Sectors – Manufacturing vs. Healthcare vs. Electric Utilities – raises Significant Questions & Highlights Multiple Problems!

The Paradox of Criticality

RSAC 2025 Conference

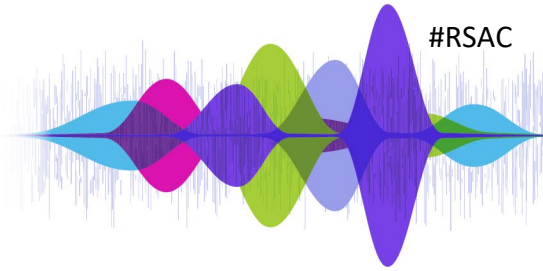
Prioritization & Resource Limitation

Decisions in Resource-Limited Environments



No Stakeholder or Decision Maker has Unlimited Resources

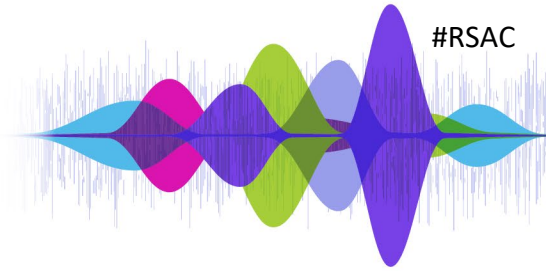
Decisions in Resource-Limited Environments



No Stakeholder or Decision Maker has Unlimited Resources

Limited Resources requires Trade-Offs & Prioritization!

Critical Infrastructure Defense Resourcing



Generally Acknowledged that Private Sector has not Sufficiently Addressed Critical Infrastructure Defense Requirements

Federal Resources - from Grants to Personnel & Capabilities - can Fill Gaps & Improve Community Defense

However - not EVERYONE can Benefit from Such Support, or Such Support Becomes Rapidly Diluted

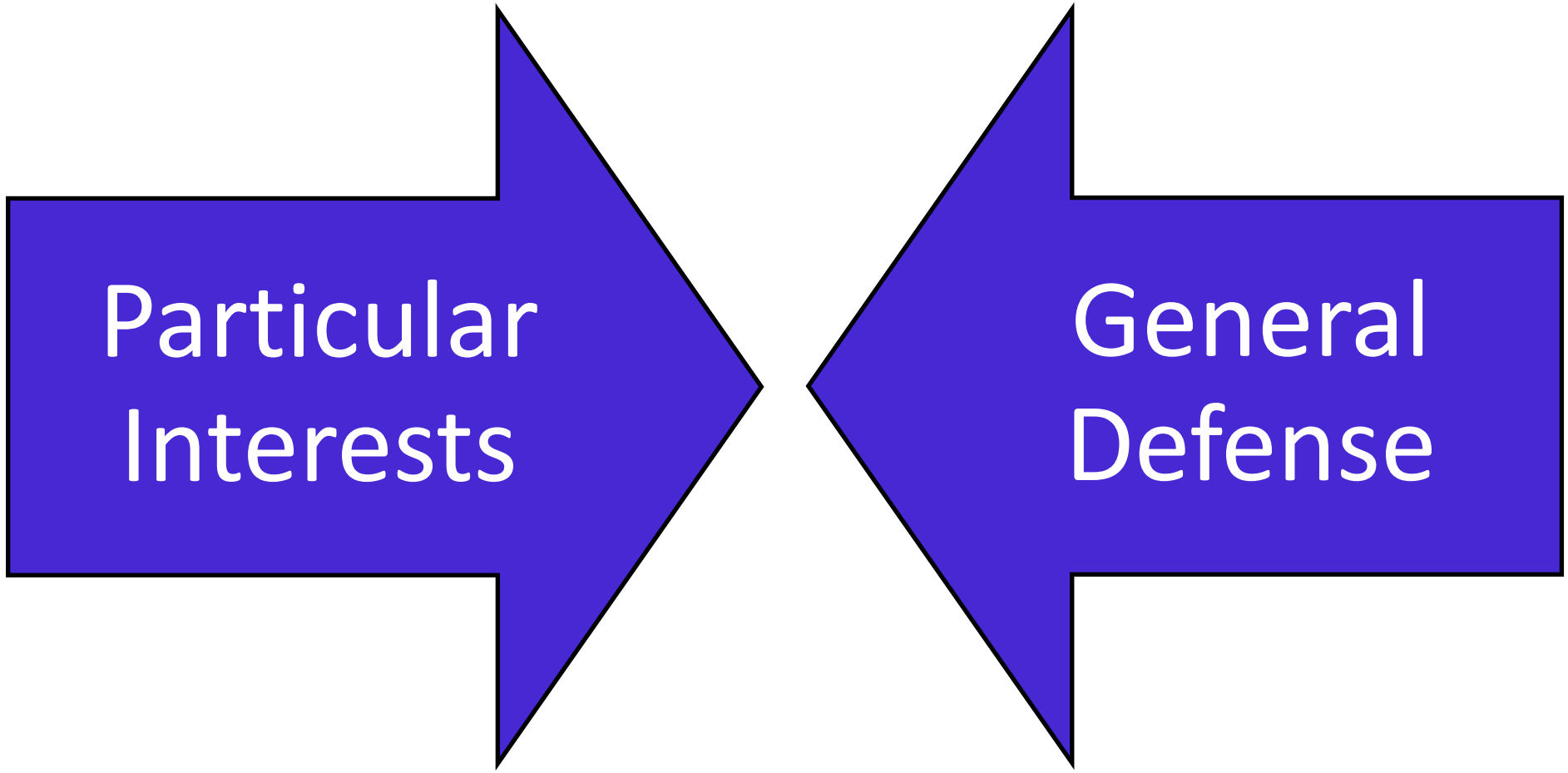
The Defender's Dilemma

Every Individual Operating Entity is Incentivized to View Themselves as "Critical"

From a National Economic Perspective, not all Things can be "Critical"

How to Balance Perspectives & Arrive at Workable Sense of "Critical?"

The Defender's Dilemma



The Defender's Dilemma

The Volt Typhoon Problem

Volt Typhoon has been Identified as a Uniquely Concerning Threat to US Critical Infrastructure

However, Volt Typhoon has Opportunistically Targeted Multiple Small Entities in Strategic Geographies

The Threat is "Macro," but the Impacts are "Micro" in Nature!

RSAC 2025 Conference

Answering the “Hard” Questions

The Essence of Strategy

Key Considerations

Critical Infrastructure Defense MUST Prioritize those Entities of Primary Military or Economic Importance!

Key Considerations

Critical Infrastructure Defense MUST Prioritize those Entities of Primary Military or Economic Importance!

Implies that SOME ENTITIES Will BE left to Fend for Themselves!

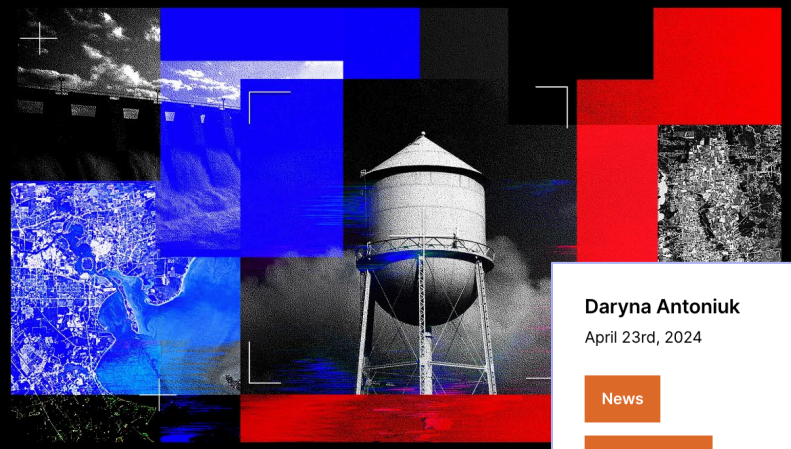
What Matters?

WIRED SECURITY POLITICS GEAR BACKCHANNEL BUSINESS SCIENCE CULTURE IDEAS MERCH SIGN IN

BY ANDY GREENBERG SECURITY APR 17, 2024 6:00 AM

Hackers Linked to Russia's Military Claim Credit for Sabotaging US Water Utilities

Cyber Army of Russia Reborn, a group with ties to the Kremlin's Sandworm unit, is crossing lines even that notorious cyberwarfare unit wouldn't dare to.



https://www.wired.com/story/cyber-army-of-russia-reborn-sandworm-us-cyberattacks/

https://therecord.media/russia-hackers-cyberattack-tipton-indiana

Daryna Antoniuk

April 23rd, 2024

News

Nation-state

Russian hackers claim cyberattack on Indiana water plant

A Russia-linked hacker group has claimed responsibility for a cyberattack on a water and wastewater treatment plant in Indiana.

The threat actor known as the Cyber Army of Russia posted a video on its Telegram channel over the weekend showing how the hackers allegedly interacted with the systems of the Tipton Wastewater Treatment Plant.

The group hasn't published any other details about the hack, but an Indiana official told CNN that the plant had indeed been a victim of a cyberattack on Friday evening, "prompting plant managers to send maintenance personnel to investigate the suspicious activity."

The general manager of Tipton Municipal Utilities (TMU), Jim Ankrum, said in a comment to CNN that the facility was targeted but hasn't been compromised.

"TMU experienced minimal disruption and remained operational at all times," he said.

Get more insights with the Recorded Future Intelligence Cloud.

Learn more.

What Matters?

VOA

Ransomware Attacks: Death Threats, Endangered Patients and Millions of Dollars in Damages

https://www.voanews.com/a/ransomware-attacks-death-threats-endangered-patients-and-millions-of-dollars-in-damages/7520952.html

https://www.npr.org/2024/06/19/nx-s1-5010219/ascension-hospital-ransomware-attack-care-lapses

npr

NEWSLETTERS SIGN IN NPR SHOP

NEWS CULTURE MUSIC PODCASTS & SHOWS SEARCH

NATIONAL

Cyberattack led to harrowing lapses at Ascension hospitals, clinicians say

JUNE 19, 2024 · 5:00 AM ET

FROM KFF Health News

HEARD ON MORNING EDITION

By Rachana Pradhan, Kate Wells

3-Minute Listen + PLAYLIST TRANSCRIPT ···

What Matters?

Defense One

About | Newsletters | Podcast | Insights | Ad

THREATS POLICY BUSINESS SCIENCE & TECH SERVICES

SCIENCE & TECH

Attacks against defense industrial base increasing, NSA chief warns

The Pentagon is pushing ahead with zero-trust plans to automate defenses against future threats.

BALTIMORE—China, Russia, and others are taking aim m
companies that serve the U.S. military, Gen. Timothy Hau
Cyber Command and the National Security Agency, told t
Cyber on Tuesday.

https://www.defenseone.com/technology/2024/06/attacks-against-defense-industrial-base-increasing-nsa-chief-warns/397652/

https://www.hydro.com/en/global/media/on-the-agenda/cyber-attack/

Hydro Aluminium Energy

Insights Contact us | You are now on our Global site

Sustainability Careers Investors Media About Hydro

Media / Topics / Cyber-attack on Hydro

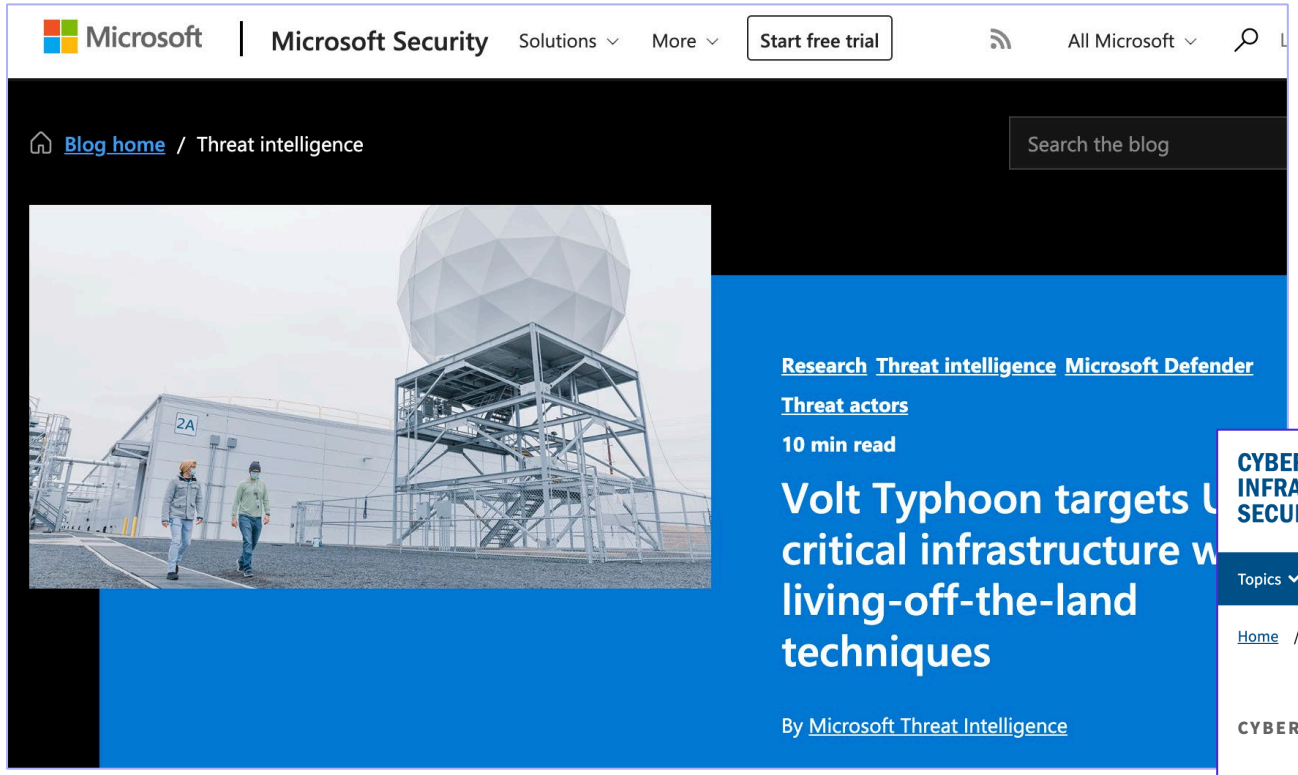
Media

- Media contacts
- News
- Hydro at a glance
- Topics
  - Cyber-attack on Hydro
  - Karmøy technology

Cyber-attack on Hydro

Hydro became victim of an extensive cyber-attack in the early hours of Tuesday, March 19, 2019, impacting operations in several of the company's business areas.

What Matters?



https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

What is in Scope?

this title.

(4) Covered entity

The term ''covered entity'' means an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant to section 681b(b) of this title.

(5) Cyber incident

https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

I. COVERED ENTITY

Covered entity is a key term in the proposed regulation as, among other things, it is the operative term used to describe the regulated parties responsible for complying with the covered cyber incident and ransom payment reporting and data and records preservation requirements in the proposed CIRCIA regulation. While the statute includes a definition for the term covered entity, the statute explicitly requires CISA to further clarify the meaning of that term through description in the CIRCIA rulemaking. Specifically, the statute defines covered entity to mean "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant to section 681b(b) of this title." 6 U.S.C. 681(4). CIRCIA also requires CISA to include a "clear description of the types of entities that constitute covered entities" in the final rule based on various specified factors. 6 U.S.C. 681b(c)(1).

What is in Scope?

Broad definition of 'covered entities'

The NPRM states that "CISA interprets the word 'entity' to be a broad term, generally including any person, partnership, business, association, corporation, or other organization (whether for-profit, not-for-profit, nonprofit, or government)," and "[t]he organizational structure or nomenclature chosen by the entity does not matter as long as it is a structure that imports legal presence or standing in the United States." While **initial reactions to the proposed rule** raise concerns that smaller entities will be exempt from CIRCIA requirements (and note the importance smaller entities have in the functioning of US critical infrastructure), the text of the proposed rule indicates that a smaller entity will be subject to the regulations if it exceeds the "small business size standard" as defined by 13 Code of Federal Regulations Part 121 **and** meets certain sector-based criteria that we describe below.

CISA's statutory mandate covers entities within **16 critical infrastructure sectors**. The CIRCIA rule understandably tracks this mandate, applying to a broad swath of "covered entities" that must operate within one of the 16 critical infrastructure sectors **and** either exceed the small business size requirement **or** meet certain sector-based criteria.

https://cdp.cooley.com/cisa-opens-notice-and-comment-process-on-circia-draft-regulations/)

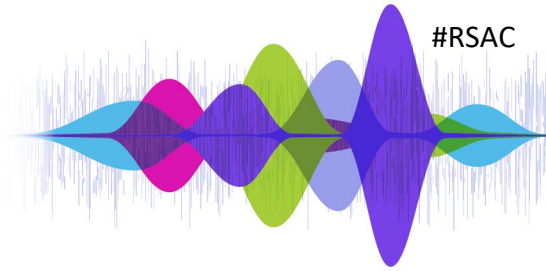
Missing the Mark?

Definition of Critical Entities is Broad so as not to "Miss" Anything

In Doing so the Scope of the Problem has Expanded too Far

Can We Economize on "Critical" & if so, How?

Answering the Hard Questions



Economic Significance

- How Vital Is a Given Resource to Continued Economic Sustainability?
- If a Given Resource is Lost, What is the Broad Economic (and Social) Impact?

Military Value

- What Purpose Does a Given Resource Serve in Enabling Military Readiness & Response?
- What Defensive Liability Exists if a Given Resource is no Longer Functional or Available?

Answering the Hard Questions

Prioritization is NECESSARY to Prevent Diluted Response

Identifying Truly Critical Entities May be Difficult but Cannot be Avoided

Result: Some "Critical" Services & Entities May be Left Behind!

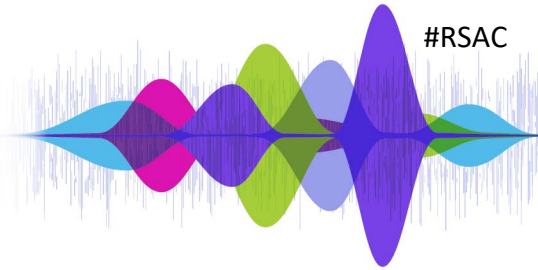
RSAC 2025 Conference

Enabling Those Left Behind

Cyber Defense & Ethics

It is <u>Ethically</u> INDEFENSIBLE to cast aside Co-Ops, Muni's, Local Hospitals, & Similar Entities Serving Non-Trivial Populations!

Cyber Defense & Ethics



It Is <u>Ethically</u> INDEFENSIBLE to cast aside Co-Ops, Muni's, Local Hospitals, & Similar Entities Serving Non-Trivial Populations!

Yet Limited Resources DEMAND that Hard Choices be Made!

Cyber Defense & Ethics

It Is <u>Ethically</u> INDEFENSIBLE to cast aside Co-Ops, Muni's, Local Hospitals, & Similar Entities Serving Non-Trivial Populations!

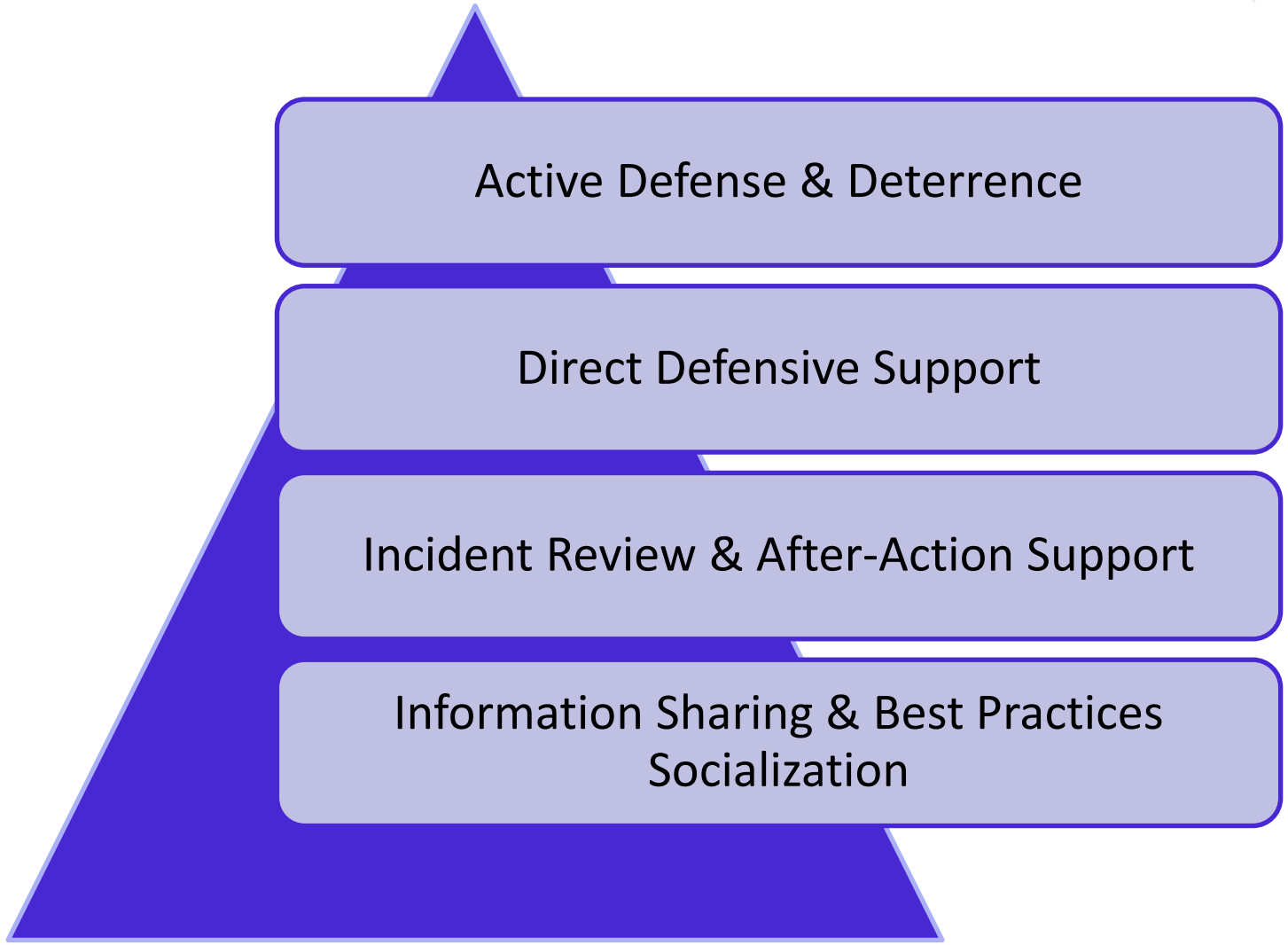
Yet Limited Resources DEMAND that Hard Choices be Made!

What Is To Be Done?

Enabling Collective Defense

- Multiple Options for Improving Defense Across Critical Entities
- Different Investments are Suitable or Desirable for Different Entities
- Prioritization doesn't Necessarily Mean ABANDONMENT

Tiered Options


Active Defense & Deterrence
Direct Defensive Support
Incident Review & After-Action Support
Information Sharing & Best Practices Socialization

Extending Defense

Diversity & Extent of "Non-Critical" Critical Entities
Mean "Direct" Investments are Difficult to Execute

However - Raising the Bar for All through
Guidance, Advice, & Support may be Attainable

Not Everyone Justifies Direct, Hands-On Support,
but Other Options Exist to Extend Defense

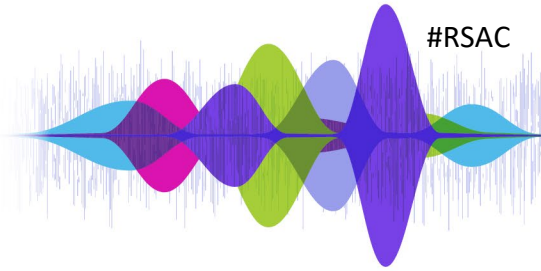
Preparing a Solution Mixture

Policy Makers & Leadership MUST be HONEST with "Non-Critical" Infrastructure Owners

Provide what Support They can, but Acknowledge Limitations to Enable Appropriate Planning

Greater Responsibility for Defense is Delegated Transparently

Economic Options to Reduce Risk



Attack Surface Reduction

Asset Inventory

Patch Management Improvement

DRP & BCP Extension

RSAC 2025 Conference

Conclusions

Difficult Choices!

Defending ALL "Critical" Items Equally Dilutes Resources, Lessens Capability

Focusing on Core Capabilities & Support Functions is Necessary

Organizations Need to be Aware of Where They Fall in this Prioritization

Shifting Responsibilities?

45 | 47

PRESIDENTIAL ACTIONS

Achieving Efficiency Through State and Local Preparedness

The White House | March 19, 2025

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

Section 1. Purpose. Commonsense approaches and investments by State and local governments across American infrastructure will enhance national security and create a more resilient Nation. Federal policy must rightly recognize that preparedness is most effectively

https://www.whitehouse.gov/presidential-actions/2025/03/test/

Shifting Responsibilities?

45 | 47

PRESIDENTIAL ACTIONS

Achieving Efficiency T
State and Local Prepar

The White House | March 19, 2025

By the authority vested in me as President by the Constitution and
States of America, it is hereby ordered:

Section 1. Purpose. Commonsense approaches and investments by
governments across American infrastructure will enhance national
resilient Nation. Federal policy must rightly recognize that prepared

https://www.whitehouse.gov/presidential-actions/2025/03/test/

https://www.wsj.com/articles/trump-administration-begins-shifting-cyberattack-response-to-states-e31bb54a

THE WALL STREET JOURNAL.

English Edition | Print Edition | Video | Audio | Latest Headlines | More

Latest World Business U.S. Politics Economy Tech Markets & Finance Opinion Arts Lifestyle Real Estate Personal Finance Health Style Sports

WSJ PRO

Cybersecurity

Home News Research Archive Newsletters Events

WSJ PRO

Trump Administration Begins Shifting Cyberattack Response to States

Preparation for hacks, including from U.S. adversaries, should be handled largely at the local level, executive order says

By Angus Loten and James Rundle

March 21, 2025 3:27 pm ET | WSJ PRO

Alternative Approaches?

Alternative Perspective: Why not Force Large Infrastructure Operators to do More?

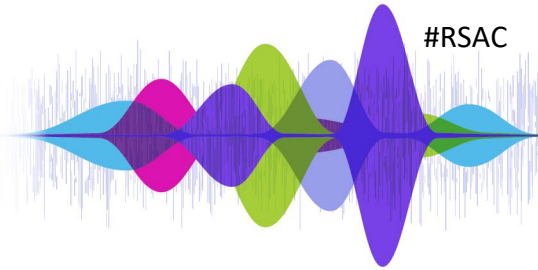
Systemically Important Entities can Shoulder a Greater Burden Outside Public Support

Public Resources Directed to Those Unable to Help Themselves

More Fundamental Questions

Where do Responsibilities Align in Critical Infrastructure Defense Between Private Sector Owners & Government Authorities?

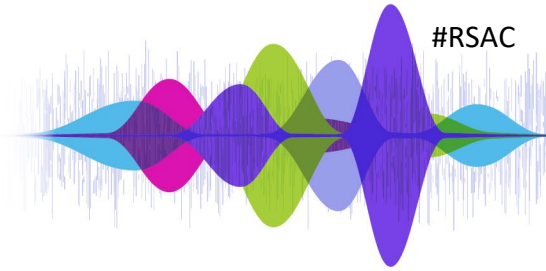
More Fundamental Questions



Where do Responsibilities Align in Critical Infrastructure Defense Between Private Sector Owners & Government Authorities?

This Needs to be Considered – but at Present, Uncomfortable Decisions are Necessary in the Current Environment!

Applications & Next Steps



Asset Owners	• Understand Where You Fall in Terms of "Criticality!" • Adapt & Adjust Defensive Plans in Recognition of Available Support!
Policy Makers	• Clearly Communicate to Asset Owners Their Priority • Adapt & Develop Plans That Allow for "Whole Of Sector" Defense at Varying Levels of Support
Commercial Vendors	• Understand Various Markets & Capacities • Adapt Products & Offerings to Meet Various Criteria & Resourcing Positions

RSAC™ 2025 Conference

Resources

Selected Resources

- *"Critical Infrastructure Systems" – CISA (https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/resilience-services/infrastructure-dependency-primer/learn/critical-infrastructure-systems)*
- *"Volt Typhoon targets US critical infrastructure with living-off-the-land techniques" – Microsoft Threat Intelligence (https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/)*
- *"PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure" – CISA (https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a)*
- *"Russia-linked hacking group suspected of carrying out cyberattack on Texas water facility, cybersecurity firm says" – Sean Lyngaas, CNN (https://www.cnn.com/2024/04/17/politics/russia-hacking-group-suspected-texas-water-cyberattack/index.html)*
- *"Hackers Linked to Russia's Military Claim Credit for Sabotaging US Water Utilities – Andy Greenberg, Wired (https://www.wired.com/story/cyber-army-of-russia-reborn-sandworm-us-cyberattacks/)*
- *"CISA Opens Notice & Comment Process On CIRCIA Draft Regulations" – Cooley (https://cdp.cooley.com/cisa-opens-notice-and-comment-process-on-circia-draft-regulations/)*

RSAC 2025 Conference

Questions?

Many Voices.
One Community.

RSAC 2025 Conference

Many Voices.
One Community.

Thank You For Attending!

For More Information:

joe@paralus.co

BSKY: @pylos.co